The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/09/2017

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Code Execution (APSB17-15)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player, the most severe of which could allow for code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Adobe Flash Player Desktop Runtime (Windows and Linux) versions 25.0.0.171 and earlier
- Adobe Flash Player Desktop Runtime (Macintosh) versions 25.0.0.163 and earlier
- Adobe Flash Player for Google Chrome versions 25.0.0.148 and earlier
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 versions 25.0.0.148 and earlier

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Adobe Flash Player is prone to multiple vulnerabilities, the most severe of which could allow for code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. The vulnerabilities are as follows:

- A use-after-free vulnerability that could lead to code execution (CVE-2017-3071).
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2017-3068, CVE-2017-3069, CVE-2017-3070, CVE-2017-3072, CVE-2017-3073, CVE-2017-3074).

Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Adobe:

https://helpx.adobe.com/security/products/flash-player/apsb17-15.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3068
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3069
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3070
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3071
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3072
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3073
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3074

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/